1-1-2015

El papel del auditor frente a una auditoria sobre TIC

Neyiredth Cuellar Triana
Universidad de La Salle, Bogotá

Olga María Pinilla Castañeda
Universidad de La Salle, Bogotá

EL PAPEL DEL AUDITOR FRENTE A UNA AUDITORIA SOBRE TIC

Neyiredth Cuellar Triana[1]
Olga María Pinilla Castañeda[2]

RESUMEN

En los últimos años los avances tecnológicos han revolucionado todos los sectores económicos y productivos del mundo, generando así que los procesos de auditoria avancen, evolucionen y se modernicen al mismo ritmo que permite lograr óptimos resultados al momento de su ejecución; el punto de la auditoría que no solo abarcará la documentación física sino también la digital generando la necesidad en los auditores de conocer y manejar las herramientas tecnologías de la información y las comunicaciones, el papel que desempeñan en la empresa.

Al realizar la auditoria de TIC es necesario conocer la normatividad, los controles y prácticas, para ello se deben conocer los contenidos de: COSO, SAC, NIAS, COBIT, ITL, ISO 27000, Las Normas de Auditoría de la Organización Internacional de Entidades Fiscalizadoras (INTOSAI), las Normas de Trabajo relacionadas a la auditoria de sistemas. En cada una de las fases de auditoría se debe estar al tanto de los marcos de referencia existentes que se deben aplicar, pues contribuiría al éxito de la misma.

La capacitación, experiencia y habilidad del auditor juegan un papel muy importante en la ejecución de la auditoria, contribuyendo con ideas y recomendaciones a la administración, las que pueden generaran mejoras significativas en los procedimientos.

PALABRAS CLAVES

Auditoria, estándares, evidencia, información, planificación, Tecnología de Información y comunicaciones.

Este artículo se realiza como modalidad de grado para optar el título de Contador Público en la Universidad de La Salle, Bogotá. Las autoras agradecen la revisión, apoyo y comentarios de la profesora Jacqueline Ovalle Pineda.

1, Estudiante de Contaduría Pública en la Universidad de la Salle Bogotá-Colombia, Analista Contable en Codelca S.A.S.

2, Estudiante de Contaduría Pública en la Universidad de la Salle Bogotá-Colombia, Administradora en Joyería Sol de Plata & Asociados.

ABSTRACT

In recent years, technological advances have revolutionized all economic and productive sectors of the world, thus generating the audit process forward, evolve and modernize at the same rate that achieves optimal results at the time of execution; the point of the audit will cover not only physical but also digital documentation generated in the auditors need to know and use the tools and information technology and communications, role in the company.

By performing the audit of TIC it is necessary to know the regulations, the controls and practices for this we must know the contents of: COSO, SAC, NIAS, COBIT, ITL, ISO 27000, Auditing Standards of the International Organization of Supreme Audit Institutions (INTOSAI), the Labor Standards related to auditing systems. In each of the phases of audit should be aware of the existing frameworks to be applied, it would contribute to the success of it.

Training, experience and skill of the auditor plays a very important role in the implementation of the audit, contributing ideas and recommendations to management, which can generate significant improvements in procedures.

KEYWORDS

Audit standards, evidence, information, planning, information technology and communications.

INTRODUCCIÓN

El área de tecnología y comunicaciones ha logrado ocupar un lugar importante dentro del organigrama de las empresas en los últimos años, la necesidad de tener la información sistematiza y controlada, los avances tecnológicos y facilidad de acceso la han convertido en una herramienta básica e indispensable dentro del mundo de hoy, por los gigantescos pasos con los que han tenido que avanzar para lograr que las comunicaciones y los sistemas de información estén al mismo nivel del crecimiento comercial y financiero de las empresas; alrededor del mundo se han logrado innumerables innovaciones y mejoras continuas con las que hoy en día podemos disponer.

La información digital se ha convertido en un elemento importante dentro de las organizaciones, de allí la calidad, veracidad y oportunidad de la misma, para facilitar la toma de decisiones y correcta disposición de la información.

Para que la información sea de calidad y confiabilidad dentro de la organización, es necesario programar auditorías a los sistemas de información y comunicación de manera

periódica, ya que mediante esta se logran los controles adecuados para obtener la confiabilidad en los sistemas y poder contar con niveles óptimos de seguridad, la auditoría verifica los registros y las fuentes para determinar si la información está acorde con lo presentado por la empresa, es importante que las tecnologías y las comunicaciones se estén ejecutando correctamente, manteniendo los controles contemplados por la empresa.

La manera como el auditor presente los resultados de sus hallazgos es fundamental para lograr que algo ocurra al interior de la empresa con la auditoría. El informe debe incluir todas aquellas acciones de oportunidad de mejora con el fin de obtener las acciones adecuadas y para lo cual el auditor debe acudir a su experiencia y conocimiento en los procesos para emitir los mejores conceptos. Una mala decisión de las acciones a tomar, en vez de ayudar a la mejora pudiera perjudicar y afectar el proceder de la empresa. El uso de los reportes de no conformidad, observaciones, oportunidades de mejora, serán de gran utilidad para la administración y su toma de decisiones enfocados hacia la mejora continua de los procesos auditados.

La evolución en el campo tecnológico y de las comunicaciones han generado cambios significativos al interior de las empresas, lo cual se ve reflejado en la prestación del servicio y en la forma como ofrecen sus productos al mercado; esto les permite optimizar los recursos y la generación de mayor productividad en los procesos, los cuales les permiten mejorar la calidad y atención a sus clientes, así mismo minimizar los recursos que se invierten, les ha generado mejores resultados y les da la oportunidad de abrir nuevos mercados a nivel nacional e internacional, donde pueden acceder a mejores oportunidades con mayor facilidad y óptimos resultados.

Actualmente no solo se deben auditar registros escritos, es importante conocer y tener control de los procedimientos que se llevan a cabo al interior de la empresa en materia de sistemas**,** para garantizar la protección y correcta manipulación de la información, para que esta no corra el riesgo de caer en manos inescrupulosas que fácilmente pueden ocasionar la quiebra en cualquier organización, se debe prevenir que los llamados Hackers puedan obtener de forma inadecuada las bases de datos tan importantes como listas de clientes o proveedores y ser utilizados para fines lucrativos poniendo en riesgo la privacidad de la organización.

Qué es la auditoria a las TIC?

La auditoría a las TIC (Tecnologías de Información y las comunicaciones), está basada en una evaluación objetiva, selectiva, crítica y sistemática de las políticas, procesos, normas, funciones, actividades de la empresa con el fin de generar un informe del uso eficiente de los recursos informáticos, de la comunicación, la oportunidad en la entrega de

la información, aprovechamiento de los recursos y la efectividad de los controles establecidos por el área de Tecnologia al interior de la empresa.

Para obtener óptimos resultado durante la ejecución de la auditoria el auditor de TIC debe contar con un conocimiento pleno frente a las Tecnologia y Comunicaciones para que pueda tener claridad en los criterios al momento de planear y desarrollar la auditoría al interior de la empresa y hacer uso de su experiencia para dar un enfoque adecuado y obtener con esto los objetivo planteados al momento de programar la realización de la auditoría de TIC.

Al momento de elegir el auditor, este debe contar con la capacidad de implementar procedimientos a través de los cuales se pueda hacer una rigurosa verificación de los recursos tecnológicos y de comunicación, la confidencialidad, integridad, disponibilidad, y confiabilidad de la información que es generada mediante los programas que se ejecutan de manera automática, buscando garantizar los resultados que serán entregados en el informe de auditoría donde los administradores y directivos podrán contar con una medición más exacta de la eficiencia y eficacia de la tecnología y la comunicación al interior de la empresa.

Normatividad que el auditor debe tener en cuenta al momento de realizar la auditoria de TIC

El auditor debe seguir los lineamientos, prácticas y controles que se encuentran contenidos dentro de los estándares y la normatividad que es relacionada en el enfoque COSO, COBIT, NIAS, SAC, ITL, los estándares de seguridad de la información (ISO 27000) entre algunos otros al momento de ejecutar la auditoría de las TIC, que hacen referencia en la realización de buenas prácticas de auditoría a los sistemas de información y comunicaciones, el control establecido para el acceso a los sistemas por parte de los funcionarios de la organización, las bases de datos donde se almacena la información procesada, la adaptación y ubicación de las áreas de servidores, instrucciones de codificación de la información, medidas de prevención de virus, fraude, controles para la detección y mitigación de personal no autorizado por la empresa.

Según (Normas de Auditoría de la Organización Internacional de Entidades Fiscalizadoras (INTOSAI), art. 153 154 155 156 157 y 158), donde hacen referencia a la importancia de la documentación del trabajo de auditoría, teniendo mayor importancia lo señalado en el art. 156 y art. 158:

> *"Art. 156. Los auditores deben justificar documentalmente, de manera adecuada, todos los hechos relativos a la fiscalización, incluso los antecedentes, y la extensión de la planeación, del trabajo realizado y de los hechos puestos de manifiesto."; "Art. 158. El auditor debe tener en cuenta que el contenido y la*

> *disposición de los documentos de trabajo reflejan su grado de preparación, experiencia y conocimiento. Los documentos de trabajo deben ser lo suficientemente completos y detallados como para permitir a un auditor experimentado, que no haya tenido previa relación con la auditoría, descubrir a través de ellos el trabajo realizado para fundamentar las conclusiones."* (Normas de Auditoría de la Organización Internacional de Entidades Fiscalizadoras (INTOSAI)).

Cuáles son los Estándares Internacionales que el auditor debe contemplar en una Auditoría de TIC?

El auditor de las TIC, debe conocer los estándares internacionales de auditoria que le ayudan al control, operación y administración de los recursos tecnológicos y de comunicación y de los procesos documentados de las tecnologías de la información y las comunicaciones. Estos estándares tienen incidencia en el proceso y desarrollo de la auditoría, ya que han de ser implementados en las empresas de acuerdo a su necesidad de resguardo, uso y protección de la información; por la importancia de ser un activo dentro de la empresa, se debe asegurar que la información se encuentre disponible, oportuna y que sea utilizada únicamente por los empleados autorizados.

Para la ejecución de una auditoría de TIC existen normas establecidas enfocadas a la Auditoría de Sistemas de información y comunicaciones, las cuales son emitidas por el Consejo Normativo de la Asociación de Auditoría y Control de Sistemas de Información Information Systems Audit and Control Association – ISACA. (Auditoria de Gestión a las Tecnologías de Información y Comunicaciones, 2011)

El objetivo de usar ITL como metodología es brindar a la empresa estándares que ayuden a facilitar el control, operación y administración de los recursos, esta metodología es la aproximación globalmente aceptada para la administración de servicios de tecnologías de información y comunicaciones en todo el mundo; consiste en una recopilación de las mejores prácticas tanto del sector privado como del sector público que se apoya en herramientas de evaluación e implementación y proponen la realización de una revisión y reestructuración de los procesos existentes en el interior de la empresa en el caso de que estos sean requeridos (si se llegara a presentar que el nivel de eficiencia es bajo o que se presente la opción de desarrollar una forma más eficiente de realizar las cosas), lo que nos lleva a la implementación de una mejora continua.

Además propone que para cada actividad que se realice en cualquiera de las áreas de la empresa y que se encuentren relacionadas con el área de tecnología y comunicaciones se debe llevar la documentación pertinente para dejar los soportes que sean requeridos en el momento de realizar la auditoria, y en vista de que esta puede ser de gran utilidad para otros

miembros de la compañía, además es importante dejar evidencia de los registro de todos los movimientos realizados, permitiendo que en cualquier momento los usuarios estén al tanto de los cambios que se realicen.

Según el (Ministerio de Comercio, Industria y Turismo, en su Decreto 0302 del **20-02-2015),** que el artículo 5° de la Ley 1314 de 2009, señala que las normas de aseguramiento de la información son un sistema compuesto por principios, conceptos, técnicas, interpretaciones y guías, que regulan las calidades personales, el comportamiento, la ejecución del trabajo y los informes de un trabajo de aseguramiento de información. Tales normas se componen de normas éticas, normas de control de calidad de los trabajos, normas de auditoria de información financiera histórica, normas de revisión de información financiera histórica y normas de aseguramiento de la información distinta de la anterior.

Que mediante comunicaciones de fechas 17 de octubre de 2014 y del 14 de octubre de 2014, el Consejo Técnico de la Contaduría Pública, en cumplimiento del procedimiento establecido en la Ley 1314 de 2009, remitió a los Ministros de Hacienda y Crédito Público y de Comercio, Industria y Turismo, respectivamente, la propuesta normativa de las Normas de Auditoria y Aseguramiento de la información (NAI) que contiene el Código de Ética para Profesionales de la Contabilidad emitido por el IESBA; las Normas Internacionales de Auditoría (NlA), las Normas Internacionales de Control de Calidad (NlCC); las Normas Internacionales de Trabajos de Revisión (NITR); las Normas internacionales de Trabajos para Atestiguar (ISAE por sus siglas en inglés) y las Normas Internacionales de Servicios Relacionados (NISR), todas estas emitidas por el IAASB y señaló igualmente, que tras la puesta en discusión pública, en la recepción y análisis de los comentarios recibidos sobre ellas, no se identificaron aspectos de fondo que pudieran implicar la inconveniencia en su aplicación en Colombia, recomendando finalmente, la expedición de un decreto reglamentario que las ponga en vigencia.

Para el auditor también es importante tener en cuenta los métodos de evaluación del control interno, entre los que están:

- Muestreo estadístico: En el momento de realizar la evaluación de control interno, el auditor debe revisar grandes cantidades de documentos, por ello se ve obligado a realizar pruebas de carácter selectivo y así poder concluir respecto a la confiablidad de determinada operación.
- Método de cuestionario: Se basa en evaluar teniendo como base preguntas que deben ser contestadas por parte de los responsables de las áreas que se encuentran bajo revisión.
- Método narrativo: radica en la descripción al detalle de los procedimientos y las características del sistema de control interno.

- Método gráfico: Es la descripción de las estructuras de cada una de las áreas y de los procedimientos.

Dentro de los objetivos planteados por el sistema de control interno, encontramos que están enfocados hacia la investigación, desarrollo, publicación y promoción de un conjunto de objetivos de control generalmente aceptados para las tecnologías de la información, actualizados, e internacionales para el uso del día a día de las empresas, administradores, directivos y auditores. Gerentes, administradores, auditores, y usuarios obtienen beneficios con el desarrollo de COBIT porque les ayuda a entender sus sistemas de información y comunicaciones, a conocer el nivel de seguridad y el control que sea necesario para proteger los activos de su empresa mediante el desarrollo de un sistema de administración de los sistemas de tecnología de la información.

Cobit

"Su sigla en inglés se refiere a Control Objectives for Information and Related Technology y es el conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA), y el Instituto de Administración de las Tecnologías de la Información (ITGI) en 1992." (Seguridad de la Información en Colombia, 2010).

"Es un marco de referencia para la dirección de IT, así como también de herramientas de soporte que permite a la alta dirección reducir la brecha entre las necesidades de control, cuestiones técnicas y los riesgos del negocio, permite el desarrollo de políticas claras y buenas prácticas para el control de TIC en las organizaciones. Enfatiza el cumplimiento normativo, ayuda a las organizaciones a aumentar el valor obtenido de TIC, facilita su alineación y simplifica la implementación del marco de referencia de COBIT." (Seguridad de la Información en Colombia, 2010).

"El propósito de COBIT es brindar a la alta Dirección de una compañía confianza en los sistemas de información y en la información que estos produzcan, permite entender como dirigir y gestionar el uso de tales sistemas así como establecer un código de buenas prácticas a ser utilizado por los proveedores de sistemas. COBIT suministra las herramientas para supervisar todas las actividades relacionadas con IT."
(Seguridad de la Información en Colombia, 2010).

Habilidades del auditor de TIC

El auditor es la persona o el equipo de personas calificado, competente e independiente, con capacitación y capacidad de desarrollar una auditoria al interior de cualquier empresa.

Una persona calificada es aquella que cumple con una serie de requisitos; en el caso de la auditoria de Tecnologia de Información y Comunicaciones deberá contar con conocimientos legales y técnicos para poder realizar su trabajo, esos conocimientos deberán estar avalados por alguna certificación, donde se relacione la formación y conocimiento acerca de sistemas de información.

Una persona competente es aquella persona calificada que a la vez asume a cambio de sus servicios, responsabilidades y obligaciones.

Por último una persona independiente a nivel de auditoría representa una persona ajena a la labor diaria del objeto a ser auditado.

Las habilidades y destrezas que pueda tener un auditor, lograran conseguir que se pueda desenvolver con naturalidad dentro de su trabajo y sabrá a enfrentar con mayor facilidad obstáculos que se encuentre a la hora de desarrollar su trabajo. Entre esas habilidades que deben tener se pueden nombrar las siguientes:

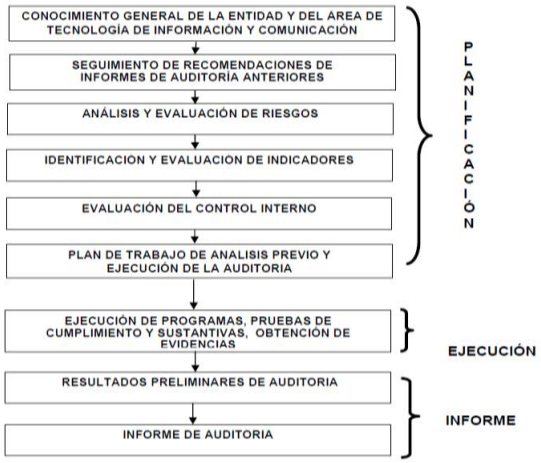
- Actitud positiva
- Saber escuchar
- Mente analítica
- Capacidad de negociación
- Iniciativa
- Facilidad de trabajar en equipo

La capacitación y la experiencia obtenida por el auditor a lo largo de su vida profesional lo llevaran a obtener mejores resultados en sus auditorías, proporcionando a la empresa fluidez y agilidad, encontrando con mayor facilidad los puntos críticos que se puedan presentar en los procedimientos establecidos por el área de TIC, logrando redactar un informe de calidad, donde la administración pueda tener conocimiento de las fortalezas y debilidades que se detecten en la auditoria.

Un buen informe presentado a la administración por el auditor podrá dar lugar a la generación de acciones de mejora que los llevara siempre en búsqueda de la implementación de cambios favorables y alcanzar las metas establecidas y tener las herramientas necesarias para que su empresa funcione cumpliendo a todos sus clientes, la administración podrá fortalecer con la opinión emitida por el auditor, su conocimiento y experiencia lo llevara a emitir sugerencias encaminadas a ofrecer ideas en la mejora de los procesos y la implementación de controles siempre con el objetivo de alcanzar los mejores resultados al interior del área de tecnología y comunicación, un beneficio en general de toda la empresa y la tranquilidad de la administración.

Planeación y Organización de la auditoria de TIC

Fases del proceso de auditoría



(Manual de Auditoría de Gestión a las Tecnologías de Información y Comunicaciones., 2011).

La planeación inicial de una auditoría al departamento de TIC, es importante para que el auditor tenga en cuenta que debe iniciar su proceso conociendo el entorno de la empresa y del área de Tecnología de la Información y Comunicaciones, cuáles son los procesos sistematizados con los que la empresa cuenta, cuál es la organización del departamento de tecnología de información y comunicaciones, los planes estratégicos que se encuentren documentados de las TIC, los planes de operación, contingencia y/o continuidad de la empresa que se encuentren relacionados con el área de tecnología de la información, la programación de los mantenimientos preventivos y correctivos de la infraestructura de los servidores y computadores al interior de la organización, esta es la mejor forma para poder establecer una adecuada planificación del trabajo que se va a desarrollar por el auditor o equipo de auditores, ese conocimiento le brinda una mayor perspectiva del marco conceptual, que le permitirá evaluar si la empresa sigue un enfoque estructurado de la gestión informática y si esta es la adecuada.

El auditor debe realizar un análisis y evaluación previa de la empresa y del área de TIC, con el fin de obtener una definición clara de las funciones, líderes del proceso y la responsabilidad de las diferentes personas que conforman el departamento de Tecnología de Información y Comunicaciones, así mismo debe analizar la ubicación dentro del organigrama de la empresa y si es recomendable que el área de tecnología de información y comunicaciones esté en un alto nivel dentro de la estructura administrativa para darle una importancia .

Una vez los auditores conozcan la empresa y el área de tecnología de información y comunicaciones, logrando identificar los asuntos que bajo su criterio sean de mayor importancia y que más llamaron su atención, deben proceder a organizarse por proyectos, deberán hacer uso de su conocimiento y análisis para la elaboración de un documento metodológico con la estrategia y alcance de la auditoría, el cuál será su evidencia de la planeación de su trabajo. A continuación datos que debe contener como mínimo la estructura de ese documento:

- Historia de la empresa y el área de TIC
- Organigrama de la empresa y del área de TIC
- Los Objetivos general y específicos de la empresa y del área de TIC
- Alcance y naturaleza de la auditoría de TIC
- Cuáles son las estrategia a utilizar en la auditoría
- Cuál es el enfoque de la auditoría de TIC
- El fundamento de la auditoría de TIC
- Se deben agrupar los asuntos de importancia examinar en la fase del análisis previo
- Cuáles son las normas a aplicar durante el proceso de la auditoría
- Con que recursos (humanos, materiales y técnicos) dispondrá el equipo de auditoría
- Cronograma de trabajo de la auditoria
- Programación de la etapa de análisis previo para iniciar la auditoría.

Como resultado de los procedimientos aplicados al conocimiento y comprensión del área de Tecnología de Información y Comunicación y de la plataforma Tecnológica de la empresa, se elaborarán programas de auditoría dirigidos a examinar lo que a criterio del equipo de auditoría les llamó la atención, con el fin de dirigir de forma adecuada los procedimientos que desarrollarán los objetivos de la auditoría.

El auditor debe verificar que el área de TIC tenga implementado y se encuentre cumpliendo con los siguientes controles:

- Que el control de toda la operación esté en manos de una misma persona
- Que las funciones de trabajo, programación y diseño de sistemas sean lo completamente claras
- Que existan los mecanismos necesarios para controlar el acceso de los usuarios, programadores y analistas para la manipulación de la información y los sistemas
- Que exista una unidad de control de calidad, tanto para los datos de entrada como para los datos de salida y los resultados del procesamiento de la información
- Que exista un adecuado manejo y custodia de los dispositivos y los archivos magnéticos, verificando que estos controles estén claramente definidos por escrito
- Todas las instrucciones de manejo del sistema deben impartirse por escrito a los usuarios

- Que exista control en el procesamiento electrónico de datos.

Así mismo debe verificar los controles existentes en las actividades del procesamiento electrónico de datos en los siguientes aspectos básicos:

Verificación de controles en el equipo de cómputo: Se debe realizar para verificar si existen formas adecuadas para la detección de errores en el procesamiento de datos, la prevención de accesos no autorizados de personal no deseado y el mantenimiento de los de los computadores, con su soporte de análisis periódicos.

Verificación de programas de ejecución: Se debe realizar para verificar que exista y se esté ejecutando un cronograma de actividades para el procesamiento electrónico de datos, asegurándose de que los computadores se estén utilizando de una manera efectiva.

Verificación de controles ambientales: Se debe realizar para verificar si todos los equipos cuentan con un ambiente adecuado, es decir si cuentan con un sistema de aire acondicionado, fuentes de energía UPS en caso de fallas eléctricas, extintores para el control incendios y las medidas que sean necesarias para garantizar la protección de los computadores y la información.

Verificación del plan de mantenimiento: Se debe realizar para verificar que todos los computadores y equipos tengan un mantenimiento adecuado que garantice su continuo funcionamiento.

Verificación del sistema de administración de archivos: Se debe realizar para verificar que exista una óptima manera para la organización de los archivos en el computador, que existan copias de respaldo, así como verificar que el uso que se da de esta información cuente con una debida autorización.

Verificación del plan de contingencias: Se debe realizar para verificar si existe un plan de contingencia apropiado que permita garantizar la continuidad en el curso de las operaciones de la empresa y la recuperación de información ante fallas humanas o eventualidades de la naturaleza que puedan poner en peligro las actividades desarrolladas, pérdida de información, infecciones en los archivos ocasionadas por virus entre otras posibles fallas que se puedan presentar en el sistema

Evaluación de los Sistemas de Información y de comunicaciones

El auditor debe realizar la evaluación de los diferentes sistemas de información y comunicación en la operación de la empresa como son (flujo de información, procesamiento de datos, manejo de la documentación, organización de los archivos físicos y magnéticos, controles informáticos y la utilización de los sistemas).

El auditor deberá verificar y asegurarse que el director del área de Tecnología de Información y Comunicaciones se ha cerciorado de que los programas adquiridos a terceros y los desarrollados internamente son la mejor opción para la empresa y van a proporcionar una efectiva y oportuna información para la toma de decisiones y se han desarrollado bajo un proceso organizado dejando todo debidamente documentado.

Evaluación de los equipos de cómputo

- Capacidades de memoria y almacenamiento
- Utilización de los recursos internos del equipo
- Nuevos Proyectos enfados a la mejora de los procesos
- Seguridad física y magnética de la información almacenada en cada uno de los equipos

El auditor debe constatarse de que el director del área de Tecnología de Información y Comunicaciones ha implementado controles al interior de su área y de toda la empresa tales como:

Controles de Adquisición: Este control garantizara que el hardware y software adquirido a terceros proporcionara los mejores beneficios a la empresa que cualquier otra alternativa analizada con antelación y garantizara la adecuada elección de equipos y sistemas de información.

El auditor debe seguir un procedimiento para velar por que esto se cumpla:

- Revisión de un informe donde el encargado de la compra justifique la adquisición del equipo, software y servicios informáticos, el cual debe incluir un estudio costo-beneficio, la ficha técnica de los equipos adquiridos y las otras opciones que tuvo en cuenta para la toma de la decisión final
- La existencia de un equipo de personas que se responsabilicen y coordine todo el proceso de adquisición e instalación de los equipos al interior de la empresa
- La existencia de un instructivo con los procedimientos a seguir para la elección y adquisición de equipos, programas y servicios informáticos. Este procedimiento debe estar ceñido a las normas y disposiciones legales vigentes
- Revisar el esquema de mantenimiento y asistencia técnica a los equipos de información y comunicaciones
- La existencia de controles para el uso del computador de escritorio y portátiles. Es una de las tareas más difícil ya que son los equipos más vulnerables, de fácil acceso, de fácil exploración por parte de personal no autorizado, los controles que se encuentren implementados deben garantizar la integridad y confidencialidad de la información.

El auditor mediante su proceso de auditoría debe asegurarse que el área de tecnología de información y comunicaciones realice los siguientes procedimientos al interior de la empresa para los computadores y servidores:

- La adquisición de equipos de protección como reguladores de voltaje y de ser posible UPS para prevenir daños eléctricos por saltos de corriente
- Programar mantenimiento preventivo y correctivo una vez se encuentre vencida la garantía de mantenimiento del proveedor del equipo
- Procedimientos establecidos para la realización de copias de soporte de la información
- Revisión del software contenido en el computador y de los informes donde se asegure que el software instalado cuente con la respectiva licencia de uso
- Revisión de la existencia de programas instalados para la detección y eliminación de virus que se puedan generar por copias no autorizadas o datos procesados en otros equipos
- Políticas que garanticen la estandarización de los sistemas operativos, software, base de datos y el mantenimiento actualizado de las respectivas versiones.

Evaluación de la Seguridad de la Información de la empresa

Los computadores y servidores de la empresa son instrumentos que procesan grandes cantidades de información, que en su gran mayoría es confidencial para la empresa y puede ser tomada para dar un mal uso o ser divulgada de manera equivocada para sacar provecho y obtener algún beneficio ilícito; además se pueden presentar que ocurran robos, fraudes o sabotajes que provoquen la destrucción total o parcial de las bases de datos que procesan la información. Esta información es de suma importancia, y al momento de la empresa no contar con ella puede ocasionar retrasos sumamente costosos y de pérdidas incalculables para la compañía.

El auditor debe verificar y constatar lo siguiente al momento de realizar la auditoria de los sistemas de información:

- Que los computadores de la empresa no tengan copias "piratas" de software y que tengan instalados software antivirus que prevengan que los computadores sean infectados al conectarse en red con otros computadores, reduciendo la posibilidad de transmisión de virus a través de la red

- Que se cuente con un procedimiento que garantice la protección del hardware y de las bases de datos procesadas, así como el control de acceso a las instalaciones del

área de servidores y de procesamiento de datos. Contemplando la posibilidad de que ocurran situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.

- La implementación de mecanismos que garanticen la seguridad del software, la protección de los datos e información y de los programas, así como la restricción de usuarios no autorizados para el acceso a la red de información de la empresa.

Indicadores de Gestión (Eficiencia, Eficacia y Efectividad) utilizados en las TIC

Los indicadores de gestión son señales que prenden las alarmas, contienen información vital que alertan si la empresa está cumpliendo en forma eficiente sus objetivos estratégicos y permiten identificar las áreas débiles de la empresa que deban ser sometidas a una acción de mejora continua o acciones preventivas que ayuden a solucionar la debilidad del área. Estos indicadores deberán ser diseñados e implementados por la compañía, el auditor es responsable de medir e interpretar los resultados obtenidos, para mejorar la gestión del área de Tecnología de la Información y Comunicaciones.

El auditor deberá evaluar el cumplimiento en la elaboración y presentación de los indicadores de gestión y a su vez desarrolla una matriz que mida los mismos, con el fin de comprobar si estos están cumpliendo con los propósitos para cuales fueron implementados.

Como debe realizar el auditor la evaluación del Riesgo Tecnológico en el área de TIC

Riesgo

El riesgo es un evento fortuito e incierto resultante de acciones humanas o por la acción de una causa externa, que puede afectar el cumplimiento de la misión, visión, objetivos y metas que han sido definidos por la empresa, causando perjuicios directos o indirectos en el desempeño diario de las funciones.

Dentro del rol del auditor durante el desarrollo de la auditoria debe realizar la verificación de que los riesgos tecnológicos han sido identificados de manera previa por el área de tecnología de información y comunicaciones, diseñando procedimientos donde se evidencie las acciones que se deben tomar en caso de la ocurrencia y el control sobre el impacto de los mismos, la probabilidad o frecuencia de que puedan ocurrir.

El auditor debe comprobar a través del análisis de riesgos que el área de tecnología de información y comunicaciones garantice de manera razonable, la confidencialidad, integridad y disponibilidad de la información tanto para el cliente interno como para el cliente externo, lo que implica establecer políticas de protección contra el uso, el acceso, la divulgación o las modificaciones no autorizadas, el daño o la pérdida o cualquier otro factor disfuncional que atente contra la seguridad de la información, tanto por parte del personal

interno como de terceros, para ello debe acatar lo establecido en las políticas y normas de seguridad de la información.

El auditor obtendrá como resultado el riesgo residual luego de realizar el análisis de riesgos, orientando su examen a las acciones de mejora tomadas por la empresa para reducirlo, aceptarlo o transferirlo, implementando controles internos para mitigarlo.

El deber del auditor es solicitar al área de tecnología de información y comunicaciones la documentación donde se evidencie que se ha identificado, analizado y gestionado los riesgos tecnológicos que pueden llegar a afectar el cumplimiento de los objetivos y metas de las TIC y la entrega de servicios en la compañía.

Cuáles son los componentes del riesgo tecnológico en el área de TIC que el auditor debe contemplar al momento de la ejecución de una auditoria:

Probabilidad: Es la posibilidad de que ocurra un riesgo y de que pueda ser medido a través de la frecuencia en que ocurra, considerando que existen factores internos y externos, que puedan generar riesgo, aún sí que éste haya ocurrido.

Severidad: Es la magnitud de los efectos o consecuencias que ocasiona al interior de la empresa la ocurrencia de un riesgo.

Nivel de riesgo: Se puede obtener mediante la confrontación de la probabilidad y la severidad del riesgo mediante los controles que existen dentro de la empresa.

Riesgos de Tecnología: Debe estar asociado con la capacidad que tiene la empresa para satisfacer las necesidades actuales y futuras de los usuarios por medio de las herramientas tecnológicas, la organización y como puedan dar soporte para lograr el cumplimiento de la misión y los objetivos.

Administración de Riesgos: Es el proceso estructurado, consistente y continuo, implementado a través de toda la empresa para identificar, evaluar, medir y reportar amenazas y oportunidades que afectan el logro de los objetivos, con el fin de ofrecer soluciones y alternativas que permitan minimizar el impacto de los riesgos.

Evaluación de Control Interno Tecnológico.

El auditor debe evaluar y supervisar los controles que tiene establecido la empresa para el área de TIC, los cuales son parte integral del entorno de control interno de la compañía, proponiendo al área de Tecnología de Información y Comunicaciones herramientas y

consejos con respecto a la implementación, el diseño, la operación y la mejora de controles del área de TIC.

El sistema de control interno del área de tecnología de información y comunicaciones está conformado por controles generales tales como (organización, implementación, seguridad de programas y datos, operación del computador, seguridad de comunicaciones y sistema operativo), los cuales han sido diseñados para asegurar que los aplicativos informáticos funcionan adecuadamente y proporcione control sobre las aplicaciones instaladas en cada uno de los computadores como son (Establecer control de acceso, entrada, salida y procesos que se deben realizar con la información), los procedimientos diseñados para asegurar que las operaciones sean administradas y supervisadas acordó con el cumplimiento de los objetivos específicos de control; que la información conserve todos sus atributos y características, y que los sistemas informáticos cumplan con los objetivos para los cuales fueron diseñados.

El auditor debe asegurarse que los controles internos establecidos por la empresa, minimicen en gran proporción los riesgos encontrados durante el proceso de análisis de riesgos, siendo posible y con una menor inversión la administración de éstos, valor agregado que podría resaltar en el informe de auditoría de TIC.

El realizar una evaluación de Control Interno aportaría a la empresa herramientas que permitan la medición de la gestión del área de informática y de la cultura de esta al interior de la empresa; al área de Tecnologia de Información y Comunicaciones le brinda indicadores que miden la satisfacción de los usuarios, tanto por los aplicativos, como por el nivel de servicio que proporciona la seguridad y la administración de la plataforma tecnológica, las señales de alerta emitidas sobre las posibles fallas en el sistema de seguridad, y le brinda una retroalimentación sobre las políticas y las medidas de control, que pueden ayudar a mejorar el funcionamiento de los computadores.

Esta revisión permite a la administración o a la gerencia tomar medidas que refuercen el área de tecnología de información y comunicaciones, para que se logre el cumplimientos de sus objetivos, se cumpla con lo planteado en las estrategias del negocio, mientras que al área de tecnología de información y comunicaciones le brinda la oportunidad de definir acciones preventivas y correctivas que puedan llevarlos a adoptar alternativas de mejoramiento continuo los servicios ofrecidos al personal de la compañía.

El conocimiento, la elaboración de programas de auditoria y la evaluación al sistema de Control Interno Tecnológico, son de los factores críticos del proceso de auditoría, por este motivo es importante que el auditor de sistemas, realice una revisión y evaluación detallada del control interno en las Tecnologías de Información y Comunicación de la empresa, buscando establecer los siguientes puntos de control:

En el área de Mantenimiento y Desarrollo de los Sistemas Informáticos.

- El cumplimiento de los objetivos estratégicos y operativos de las TIC
- La operación y funcionamiento de los sistemas.
- La instalación y el uso de las aplicaciones.
- La actualización en la tecnología y los avances que se evidencien.
- La oportunidad y continuidad en la prestación del Servicio.

El auditor realizara una revisión y evaluación de las condiciones físicas y de seguridad del departamento de tecnología, que permita garantizar que las medidas de seguridad que están siendo usadas en los computadores y servidores están siendo controladas de manera tal que se revise si están cumpliendo con el objetivo para lo cual fueron diseñadas. A la evaluación se le debe dar un enfoque técnico y la implementación de una medida preventiva, para reducir el riesgo de los ataques externos e internos hacia la información de la empresa, que puede llegar a afectar la continuidad de las operaciones y entrega de información.

El auditor debe asegurarse que el sistema de control interno haya sido implementado por la administración de la empresa y sea revisado continuamente como una medida de prevención, para anticiparse a situaciones que puedan poner en peligro la información o la continuidad de las operaciones de la compañía; así como para tener conocimiento y control del tiempo de respuesta y poder buscar mejores opciones para el mejoramiento de las estrategias de TIC.

El auditor deberá obtener suficiente y apropiada evidencia mediante la ejecución de sus procedimientos, la cual le permitirá emitir su opinión y tener fundamentos al momento de elaborar el informe acerca de la operación de la gestión en el área de Tecnología de Información y Comunicaciones.

Qué es la evidencia suficiente de una auditoria de TIC

Se conoce como la cantidad y calidad de evidencia obtenida por el auditor, mediante las pruebas y evaluaciones durante el desarrollo de la auditoría, que le permitirá emitir conclusiones razonables acerca del uso de las herramientas Tecnologías de información y Comunicaciones que han sido sometidas a examen. El auditor no deberá obtener toda la evidencia que encuentre, sino seleccionar la que cumpla, utilizando su juicio profesional y que considere será la más razonable y apropiada para cumplir con el objetivo establecidos al inicio de su auditoria.

Es importante que el auditor obtenga la suficiente confianza sobre la evidencia recolectada, ya que esta debe ser más convincente que concluyente, con frecuencia los auditores buscan evidencia en diferentes lugares o de con naturaleza distinta como apoyo

de un mismo dato o un hecho. Se considera que la evidencia es adecuada cuando es utilizada finalmente por el auditor para emitir su juicio profesional de manera clara, acertada y exacta.

El auditor decidirá que procedimientos utilizara durante la auditoria para la obtener evidencia, cuáles de estos son los más convenientes durante cada instancia de esta.

Evidencia adecuada de la auditoria de TIC

El concepto de "evidencia adecuada" le proporciona una característica cualitativa, mientras que el concepto de "evidencia suficiente" le proporciona una característica cuantitativa. La reunión de los dos tipos de evidencia ayudara al auditor a obtener el conocimiento adecuado y suficiente para alcanzar bases sólidas y objetivas sobre los hechos encontrados y examinados durante la auditoria. La evidencia será considerada adecuada cuando le permita al auditor emita su juicio profesional plasmado en su dictamen.

Como se debe documentar la evidencia obtenida durante la auditoria de TIC

La evidencia recolectada durante la ejecución de la auditoria debe ser recogida mediante la elaboración de papeles de trabajo, que serán utilizados por el auditor como soporte y justificación del trabajo ejecutado y poder documentar todos aquellos asuntos de importancia que no estén conforme a la normativa técnica y legal en la operación y el uso de las TIC.

Protección y Conservación de la evidencia de la auditoria de TIC

La evidencia obtenida durante la auditoria de TIC deberá estar protegida contra el acceso no autorizado y la modificación por parte de personal ajeno al equipo de auditores.

De la misma manera debe conservarse después de finalizado el trabajo de auditoría, durante el tiempo que sea necesario para el cumplimiento de todas las leyes aplicables, reglamentos y políticas de la empresa.

Carta de Salvaguarda sobre la protección de la evidencia

Antes de que el equipo de auditoría se retire de la empresa, es fundamental que el auditor líder obtenga la carta de salvaguarda, en la que la administración relacionara la gestión del departamento de tecnología de información y comunicaciones, suscrita por el gerente de la empresa o por la persona a quien él designe, con el fin de que el equipo de auditores pueda demostrar que toda la información relacionada con las TIC solicitada, ha sido prevista por la administración de la empresa.

Procesos

Dentro de los elementos que intervienen en el proceso, el área de tecnología de información y comunicaciones deberá elaborar un plan estratégico de trabajo, definido como un documento a largo plazo que contenga la estrategia de proyectos de modernización de los procesos a través de los recursos tecnológicos, con el objetivo de brindar con calidad el servicio ofrecido a los clientes internos y externos de la empresa, y como mínimo dicho plan debe contener los siguientes alcances:

- Objetivos estratégicos
- Misión
- Visión
- Acciones estratégicas
- Cuáles son los procesos que serán automatizados
- Que usuarios intervienen en el proceso de automatización
- Recursos humanos, materiales, financieros y técnicos
- Cronograma de implementación de los proyectos

Planes de Contingencia para el área de TIC

Es un conjunto de tareas que el área de TIC debe realizar en caso de que se presenten fallas en los sistemas que impidan el funcionamiento normal de los servicios, con el fin de recuperar a la brevedad las operaciones de la empresa.

El auditor debe conocer y analizar el plan de contingencia implementado por la empresa para poder ser auditado, con el propósito de determinar el grado de efectividad y eficiencia que brinda a la continuidad de los servicios y minimizar la probabilidad y el impacto de interrupciones, funciones y procesos claves del negocio, evitando con esto que el cese de operaciones pueda ocasionar perjuicios económicos a la compañía.

El auditor debe conocer y comprender en que momento el área de TIC ha generado un requerimiento para la elaboración de procedimientos que establezcan los planes de contingencia para los servicios tecnológicos y de comunicaciones adquiridos o contratados a través de terceros con el propósito de garantizar la continuidad de las labores de la empresa, deberá supervisar los procesos de recuperación y determinar el impacto de la contingencia; para esto deberá realizar con los proveedores pruebas de contingencia para determinar la efectividad del plan de contingencia ofrecido.

Planes de Mantenimiento

El auditor deberá contar con el conocimiento necesario para poder analizar y comprender los planes de mantenimiento de la plataforma Tecnológica (hardware y software) implementado por el área de TIC, con el objetivo de verificar que la plataforma tecnológica está en la capacitada para garantizar que funcione continuamente, la oportunidad y la disponibilidad de la información.

El auditor debe conocer, comprender y analizar la estructura organizacional de la empresa de manera general, identificando las principales áreas, elementos administrativos, recursos humanos (principales funcionarios), productos y/o servicios de la compañía, así como la relación que mantiene con otras empresas y conocer las funciones del área de Tecnología de Información y Comunicaciones como son sus principales aspectos, estructura organizacional, objetivos y metas operativas, organización y función, procesos, productos y/o servicios aplicando procedimientos generales tales como:

- Revisar y evaluar si la función de TIC están sujetas a la misión, visión, valores, objetivos y estrategias de la empresa y deberá revisar el desempeño esperado por la empresa evaluando su cumplimiento
- Revisar y evaluar la eficacia de los recursos de TIC y el desempeño de los procesos administrativos
- Evaluar el riesgo de las funciones de TIC
- Revisar y evaluar el ambiente de control de la empresa
- Revisar las áreas físicas, con el propósito de verificar si está en condiciones para la operatividad de las TIC
- Revisar las funciones de cada uno de los técnicos para comprobar si estos cuentan con la capacitación y las condiciones necesarias para realizar su trabajo
- Revisar y evaluar que el Manual de funciones sea aplicable y este acorde a la realidad de las funciones del personal del área de Tecnología de Información y Comunicaciones.

El auditor debe conocer, comprender y analizar de forma general la Gestión de las TIC, la plataforma tecnológica y los sistemas de información aplicados a la empresa, tales como:

- La estación de donde se encuentren los servidores y sus características
- Cuál es la seguridad que brinda la estructura de redes
- Con que sistemas operativos cuentan los computadores
- El software y hardware instalado en cada computador
- El inventario de Hardware y Software con el propósito de establecer el nivel de obsolescencia o actualización y legalidad en la adquisición de estos por parte de la empresa

- Los servicios contratados por la empresa con terceros y que estén directamente vinculados con el área de tecnología de la información y comunicaciones
- La infraestructura eléctrica para el control de las descargas eléctricas, entre otras.

Los Papeles de Trabajo Electrónicos.

Cada empresa tiene diseñados e implementados formatos que permiten la elaboración de papeles de trabajo en medios electrónicos, los que se almacenan según las necesidades de cada empresa.

El auditor deberá preparar y conservar los papeles de trabajo de manera adecuada, los cuales le ayudaran en la planeación, supervisión, desempeño y evaluación de la auditoría, y donde quedará registrada la evidencia adecuada obtenida para apoyar la emisión de la opinión.

La documentación de la auditoría es conocida también como: "papeles de trabajo", y hace referencia al registro de los procedimientos desarrollados en la auditoría, es decir, la evidencia más relevante obtenida en el transcurso de la misma; incluyendo las conclusiones a las que llegara el auditor.

La elaboración de los papeles de trabajo electrónicos por parte de los auditores de TIC serán de manera digital y deberán contener todos los hallazgos y la evidencia recolectada durante el transcurso de la auditoria, de tal forma que muestren la información y los hechos específicos y completos, el alcance del trabajo realizado, las fuentes de la información obtenida y las respectivas conclusiones.

Para el caso de la auditoria de Tecnologia de Información y Comunicaciones el medio será electrónico y documental respecto a la evidencia de respaldo obtenida por el auditor de las deficiencias encontradas durante el proceso, la cual debe estar impresa y con los suficientes soportes.

La documentación de la auditoría debe ser preparada y archivada de tal manera que si en determinado momento otro auditor con experiencia necesite tener acceso a ella por cualquier motivo, pueda entender: la naturaleza, oportunidad y extensión de los procedimientos de auditoría desempeñados; los resultados y la evidencia obtenidos durante la auditoría, así como las conclusiones.

Los papeles de trabajo deben ser preparados con la suficiente evidencia de los hallazgos encontrados para que sean adecuados y detallados con el fin de que haya un mejor entendimiento de la auditoría.

Seguimiento a Recomendaciones de Auditorías Anteriores.

El auditor de TIC debe obtener solicitar copia de los informes de auditorías anteriores y que se encuentren relacionadas con el proceso de las tecnologías de información y comunicación, para poder realizar el seguimiento y verificación del cumplimiento de las recomendaciones asignadas en las auditorías anteriores. En este caso, el auditor solicitará a la administración los procedimientos y las acciones de mejoras implementadas para comprobar que se esté dando cumplimiento y a la evidencia que las respaldan, estas serán analizadas para establecer el grado y nivel de cumplimiento por parte de la empresa de las recomendaciones.

Al comprobar que las recomendaciones se encuentran cumplidas el auditor, comunicará por escrito los resultados del seguimiento a las personas encargadas del cumplimiento, haciendo mención que se han implementado las acciones correspondientes al mejoramiento del control interno o de la gestión tecnológica y de comunicaciones en la empresa y deberá incluir en el informe final de auditoría un párrafo estableciendo que la empresa cumplió con las recomendaciones dadas en el informe anterior de auditoria.

En caso de realizar el análisis de las acciones correctivas implementadas por la empresa, éstas no son suficientes para dar cumplimiento con las recomendaciones realizadas en el informe auditoria anterior, se deberá desarrollar un asunto de importancia, que deberá incluirse en el informe final de auditoría, en un párrafo donde haga referencia a los resultados encontrados sobre el seguimiento a las recomendaciones de la auditoría anterior; resaltando lo siguiente:

- **Identificación:** El auditor debe hacer referencia al informe y período auditado sobre el que está efectuando el seguimiento
- **Condición:** El auditor debe incluir la situación encontrada de la auditoría anterior
- **Recomendación:** El auditor debe incluir la recomendación planteada en la auditoría anterior
- **Comentarios de la administración:** El auditor debe describir la situación actual de las acciones de mejora tomadas por parte de la administración, para dar cumplir con la recomendación de la auditoria anterior
- **Grado de cumplimiento:** El auditor debe indicar el grado de cumplimiento actual por parte del área de TIC.

Conclusiones

- El auditor de TIC debe preocuparse por mantenerse actualizado permanentemente en los tema de Tecnología de la información y las Comunicaciones, dado por la rapidez de los avances tecnológicos, los procesos de auditoria no se pueden quedar relegados, al contrario deben crearse nuevos estándares y metodologías para realizar las auditorías a las empresas para así poder realizar el trabajo de manera eficiente y con la certeza de realizarlo de la mejor manera posible.

- La presentación de los resultados, opiniones y sugerencias por parte del auditor son fundamentales para lograr que la administración se basen en ellos aprovechando el conocimiento y la experiencia con la que el auditor las emite, así puedan impartir instrucciones de cambios importante y satisfactorios al interior de la empresa como resultado de una buena auditoría.

- En el marco de los avances tecnológicos se hace completamente necesario para el auditor obtener la capacitación y la experiencia para realizar auditoria a la Tecnología de la información y las Comunicaciones de las empresas, ya que en la mayoría de los casos la información es netamente digital.

- Para los auditores y las compañías es importante cumplir con cada uno de las fases y pasos para realizar la auditoria, y obtener la evidencia adecuada para la presentación del informe final.

- El papel de la administración es muy importante para establecer las acciones de mejora y las acciones correctivas a los hallazgos informados por el auditor en su dictamen final.

Apreciaciones de las autoras con respecto al tema

Enfocándonos en los avances tecnológicos y la sistematización de la mayoría de las empresas a nivel mundial, podemos apreciar que el área de tecnología de la información y comunicaciones ha logrado posicionarse en un lugar alto dentro del organigrama de las empresas, por esta razón la administración se ve en la necesidad de realizar auditorías regulares al departamento de TIC para garantizar la continuidad del negocio y el grado de respuesta a posibles eventualidades.

Es importante que la gerencia al momento de seleccionar el grupo de auditores o el auditor que va a realizar la auditoria del proceso, tenga claridad en los alcances y conocimientos de este. El papel del auditor frente a una auditoria de TIC, es clave para obtener los resultados esperados al momento de la programación de la misma.

Es importante que la capacitación y actualización del auditor frente a las TIC, se realice con la misma velocidad con que avanza la tecnología, para ir al día con los cambios y mantenerse actualizado con las nuevas normatividades, esto brindara garantía de su trabajo, la recopilación de la evidencia adecuada y necesaria la va a realizar bajo un alto criterio profesional.

De un buen informe presentado por el auditor como resultado de sus hallazgos, la administración podrá obtener información valiosa para la toma de decisiones, el informe debe incluir todas aquellas acciones de oportunidad de mejora, sugerencias y recomendaciones con el fin de facilitar a la administración una buena herramienta donde puedan obtener las acciones adecuadas y para lo cual el auditor debe hacer uso de su experiencia y conocimiento en los procesos de auditoria para emitir los mejores conceptos y que se adaptan mejor a las necesidades de la empresa auditada.

Bibliografía

"Corte de Cuentas de la República", (2011). Disponible: *"Auditoria de Gestión a las Tecnologías de Información y Comunicaciones".* El Salvador, C.A.: Recuperado, martes 17 de febrero de 2015 en: http://bibliotecavirtual.olacefs.com/gsdl/collect/guasyman/archives/HASH0155.dir/ManualAuditoriaGestionTICs.pdf

"Seguridad de la Información en Colombia", (2010). Disponible: *Noticias sobre avances en este tema que se den en nuestro País, y en general sobre cómo evoluciona este agitado mundo regido por la ISO 27000. "La seguridad es el mayor enemigo".* Colombia.: Recuperado jueves 25 de febrero de 2015 en: http://seguridadinformacioncolombia.blogspot.com/2010/07/que-es-cobit.html"

"Sistemas de Información", (2010). Disponible: "*Estándares COBIT e informe COSO".* Recuperado, viernes 6 de marzo de 2015 en: http://es.slideshare.net/Dannyadpr/estndares-cobit-e-informe-coso

"Seguridad de la información en Colombia" (2010). Disponible*: "COBIT: Governace, Control and assurance for information and related technology",* Recuperado, jueves 30 de abril de 2015 en: http://seguridadinformacioncolombia.blogspot.com.co/2010/07/que-es-cobit.html

"INTOSAI Organización Internacional de las Entidades Fiscalizadoras Superiores" Disponible: *Normas de Auditoría de la Organización Internacional de Entidades Fiscalizadoras (INTOSAI), en los artículos 153 a 158,* Recuperado, Domingo 25 de mayo de 2015 en: www.intosai.org/es/acerca-de-nosotros/issai.html

"ISACA Information Systems Audit and Control Association (Asociación de Auditoría y Control en Sistemas de Información" Disponible: *Guía de Auditoría y Aseguramiento de SI 2401 Reportes,* Recuperado, Miércoles 28 de mayo de 2015 en: http://www.isacacr.org/archivos/Acai_Normas/G20%20-Reportes_es.pdf